PKI With A Purpose

Agenda

- Introducing Keon
- Fundamental Technologies
- Keon with PKI-Ready and Non-PKI-Ready Applications
- Additional Keon Services
- Keon & SecurID
- Questions & Answers

Introducing... 

- Open, standard PKI security foundation for enterprise and E-commerce applications
- Products for both OEM and enterprise customers - from PKI components to turn-key PKI systems
- Built-in support for existing enterprise applications
- Leverages the combined power of Security Dynamics and RSA

A Comprehensive Security Foundation

- Desktop, application, network and host security
- Establishes and manages trust relationships via digital certificates
- Centralized dual key and credential management, reporting and audit
- Enables certificate use with multiple applications
- Supports SecurID strong authentication

A Range of PKI Options

- A turnkey system providing a scalable, enterprise-ready solution
- Certificate Server for developers building customized solutions
- Plus, RSA BSAFE crypto and protocol components to build native PKI applications

Application Security

- Transparently secures existing applications
  - Non-invasive application-level VPN agents
  - SDK enables custom use with existing applications
- Provides certificates for today's PKI-enabled applications
- Secure Single Sign-on

Interoperability

- Supports cryptographic and security standards
- Compatible with popular network, application and system environments
- Allows organizations to implement the CA or directory service of choice

Keon's Heritage

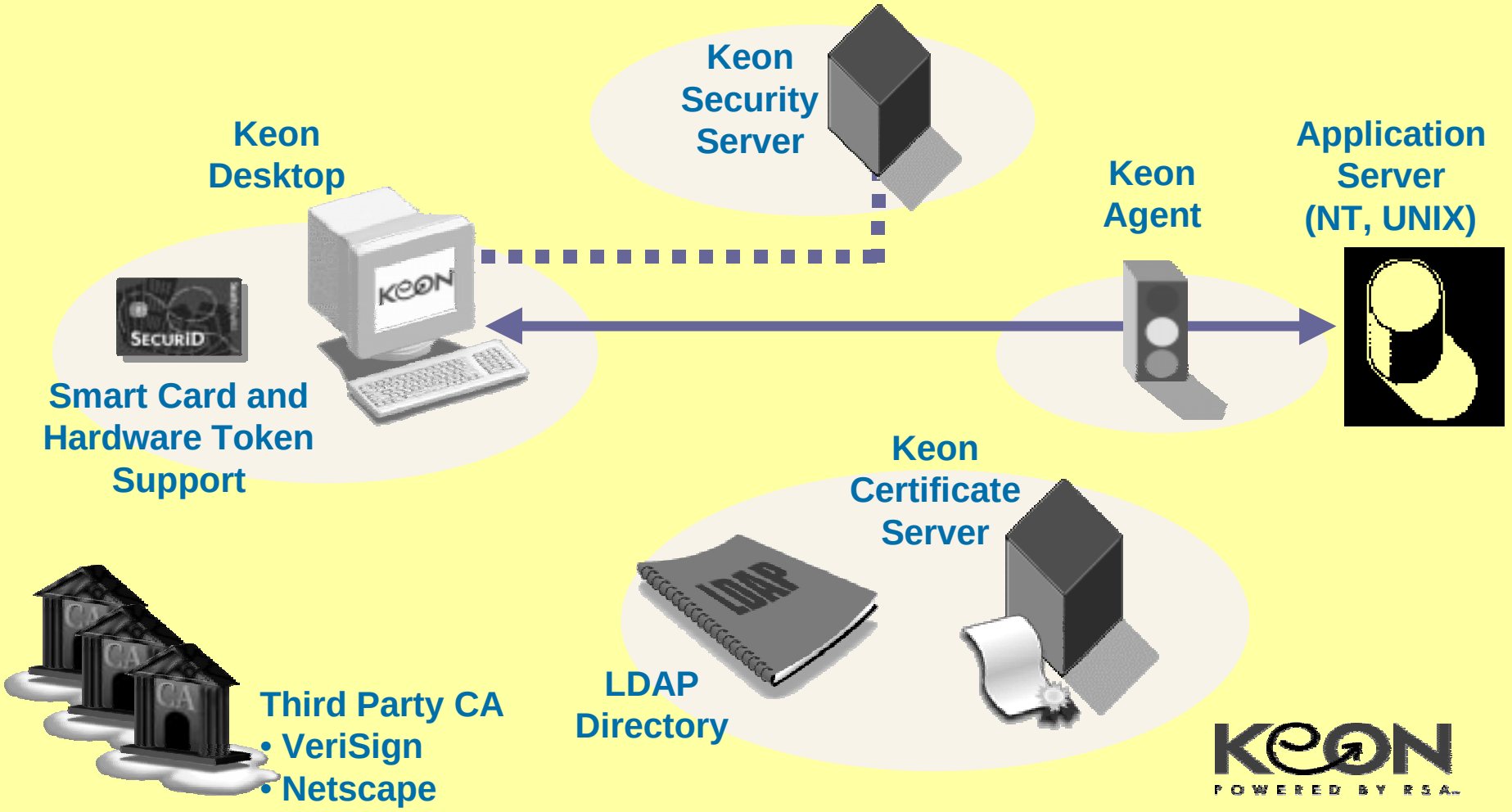
- Pioneers & undisputed leader in strong user authentication
- 15 years enterprise security systems experience
- 70% share of the strong authentication marketplace
- Developers of the BoKS product

- Pioneers and leaders in standards and practical use of public key
- 17 years providing security technology to industry
- 400,000,000+ installed worldwide
- Accelerating licensee growth

PKI Technology Issues

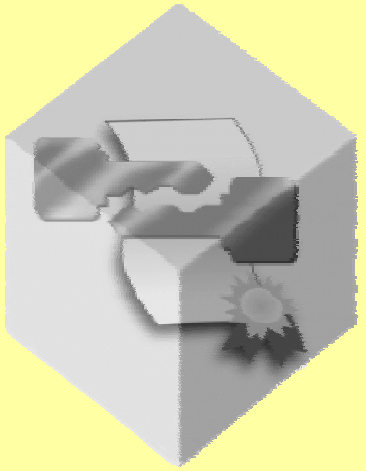
- Multiple certificate sources
- Multiple applications need to access certificates…simultaneously
- Distributing certificates to users
- Certificate and private key access …independent of location
- Authentication and Digital Credentials
- PKI-enabling applications

Keon Product Family Components



Fundamental Keon Technologies

The Keon Credential Store



- Centralized credentials
- All credential stores provide
  - Identity Certificate
  - Private keys (3DES)
  - Additional user credentials for local network (e.g. NT or NetWare - RC4 protected)
  - Secure storage of user data
- Implemented in virtual or physical smart cards

Credential Store and Life Cycle

- Shared access to single certificate and key store
- Dynamic download of credentials
  - Caching under policy control
  - Physical transfer if required
- Consistent update across all applications
- Notification of updates

Privilege Attribute Certificate (PAC)

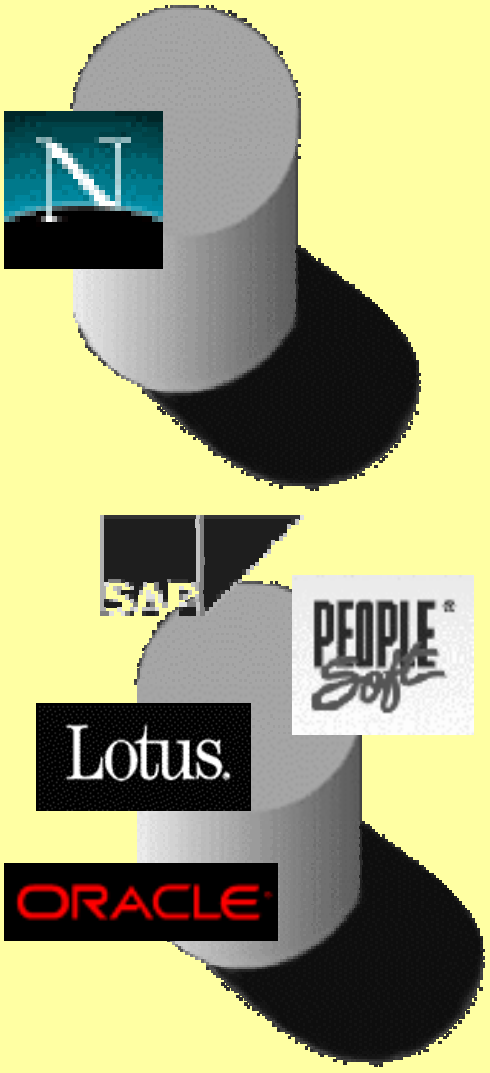
- Primary function is transport of authorization
- Provide application specific logon credentials
- X.509 Certificate generated internally
- Does not require the presence of a “real CA”
- Created when a user accesses an application
- Generated in “real time” with a short life time (24 hours or less)
- Treated like certificates internally
- Not available or seen by users

Using Keon with PKI-Ready and Non-PKI-Ready Applications

Mission Critical Apps Need Mission Critical Security

- Organizations run on information
  - Financial
  - Manufacturing/Supply Chain
  - R&D
  - M&A
- Access to applications is required from a broader set of users
  - Employees
  - Partners
  - Customers
- It has to be secure!

Keon Application Security



PKI Ready Application

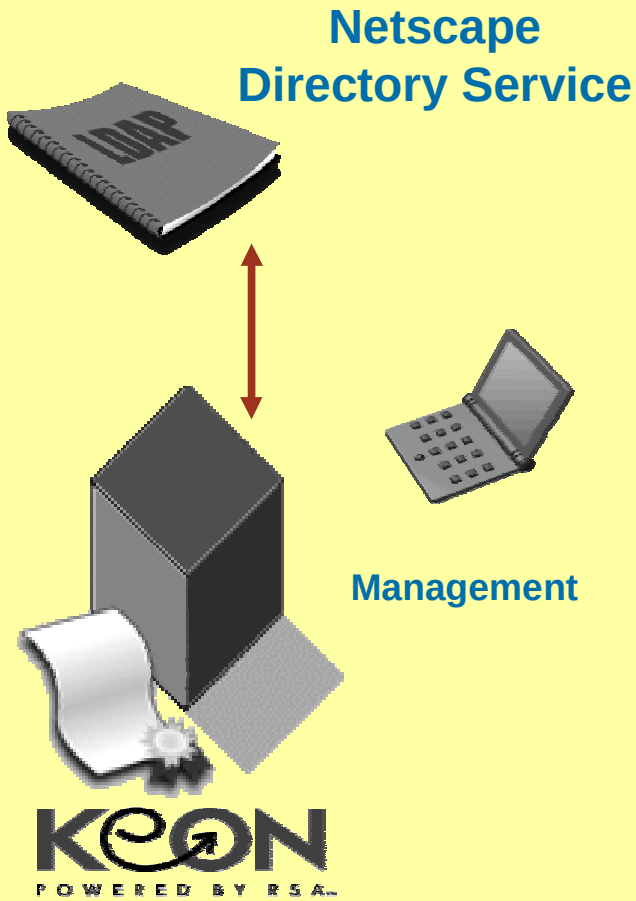
- Work with PKI “out of the box”

Non - PKI Aware Applications

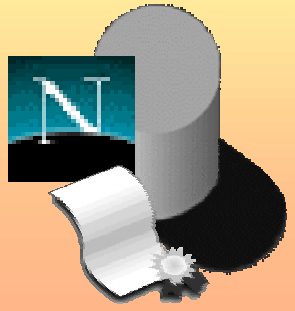
- Need to be adapted for PKI
- “Wrapped” or Embedded

Enabling Security for PKI Ready Applications

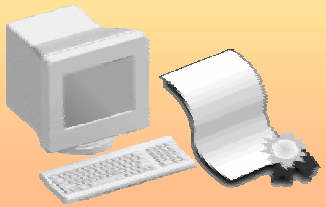
- Manage trust relationships for applications using digital certificates
- Keon Certificate Server (CA)
  - VeriSign technology engine
  - RSA enhanced for self-management
  - Netscape Directory Service option
- Flexible support for:
  - Off-the-shelf Web browsers/servers
  - Email clients
  - Custom built applications
  - IPSEC network encryption solutions



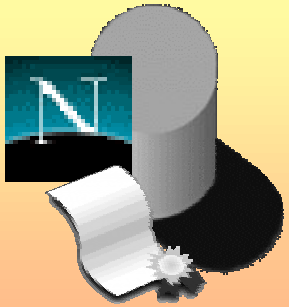
Keon Certificate Server for Web Applications



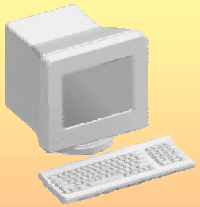
SSL Encryption



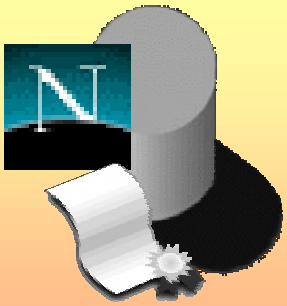
Server and Client Certificates



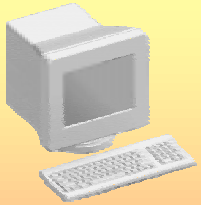
SSL Encryption



Server Side Certificates w/WebID



SSL Encryption



Weak Password Authentication

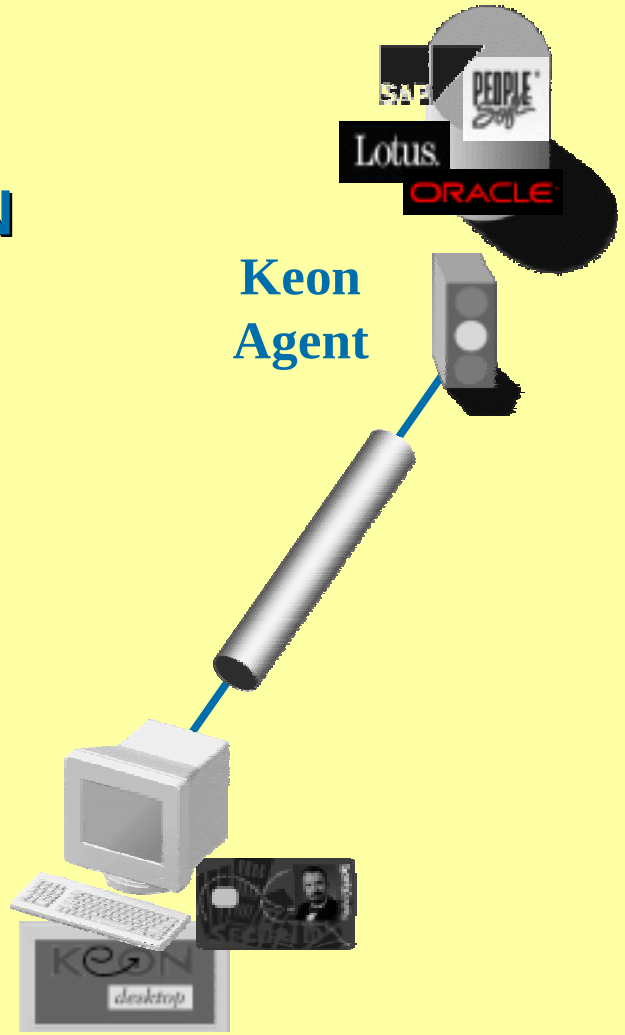
Server Side Certificates Only

The Keon Certificate Server Solution

- **Keon Certificate Server (CA)**
  - VeriSign technology engine
  - RSA enhanced for self-management
  - Netscape Directory Service option
- **Comprehensive support for:**
  - Off-the-shelf Web browsers & servers
  - Browser-based email systems
  - IPSec network encryption solutions
  - Custom PKI applications
- **“In-sourced” CA**

Enabling Security For Existing Applications

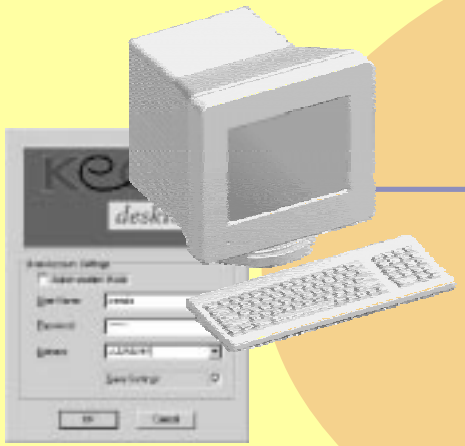
- Business information stays confidential - Application VPN
- Non-intrusive - requires no change to application
- PKI-based single sign-on to “Keon Ready” enterprise applications
  - x.509 identity certificate
- Centralized audit & reporting of authentication activity

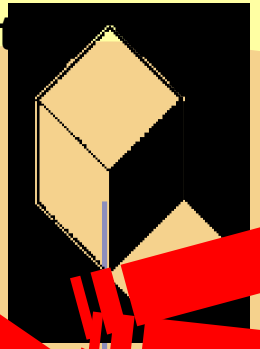


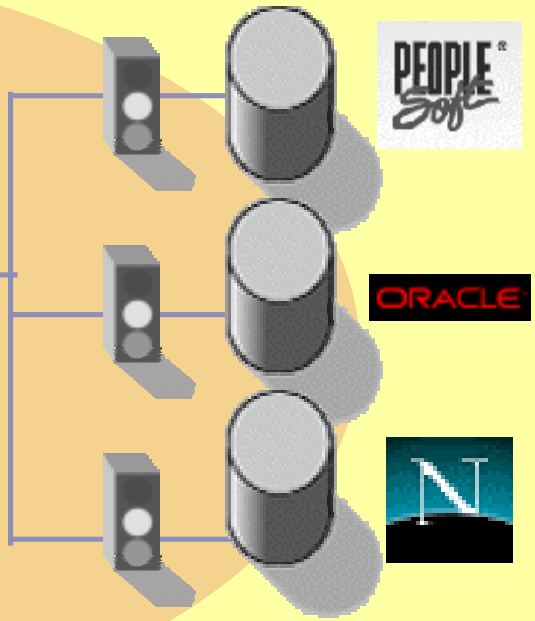
Reducing Pain & Cost of Password Management

+ Pin

Keon Securit
Server





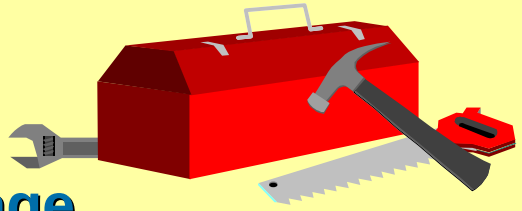


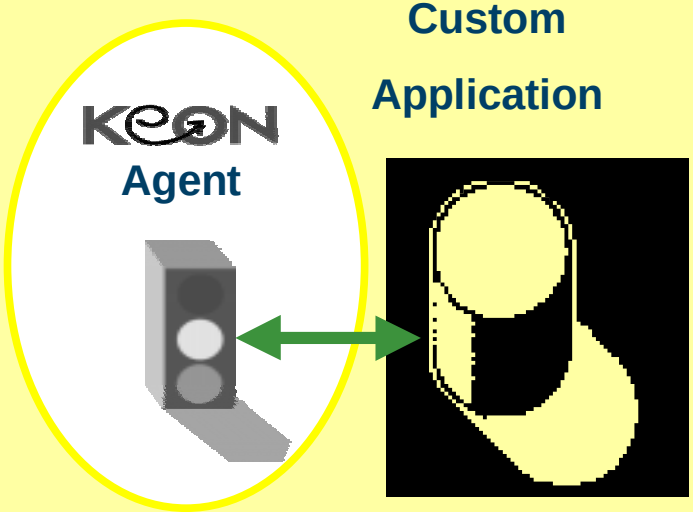
- User authenticates *once* to Keon Desktop

User:= DStorey		
app:=Oracle	pw:=ora17143	priv:=user
app:=PeopleSoft	pw:=HR	priv:=HR
app:=Web App1	pw:=SAP1943	priv:=user

Extending Keon Agent Services

- **Keon Agent SDK**
  - **Enable your legacy applications to take advantage of public key security**
  - **Non-invasive approach**
- **Keon Certified Professional Services**
  - **From Security Dynamics or partners**
  - **Work with customers to provide the solution you need for your business!**





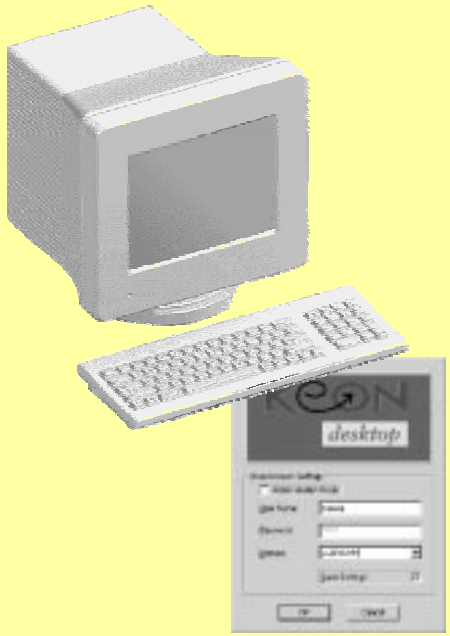
Building Interoperable PKI Ready Applications

- BSAFE SSL & S/MIME pre-built for PKI; BSAFE Cert-C coming soon
- One stop development platform
  - Client and server-side tools
  - Keon Certificate server and LDAP server
- "Component" approach providing interoperable, standards-based technology
  - Keon Certificate Server or VeriSign On-Site certified at FCS, others later
- RSA's core value proposition

Keon Desktop

PKI-based Desktop Security System

- Physical or virtual smart card protection & credentials
- X.509 certificates
- Transparent encryption for local and network files
- Roving Credentials/Free Seating
- Automated login into NT and Netware



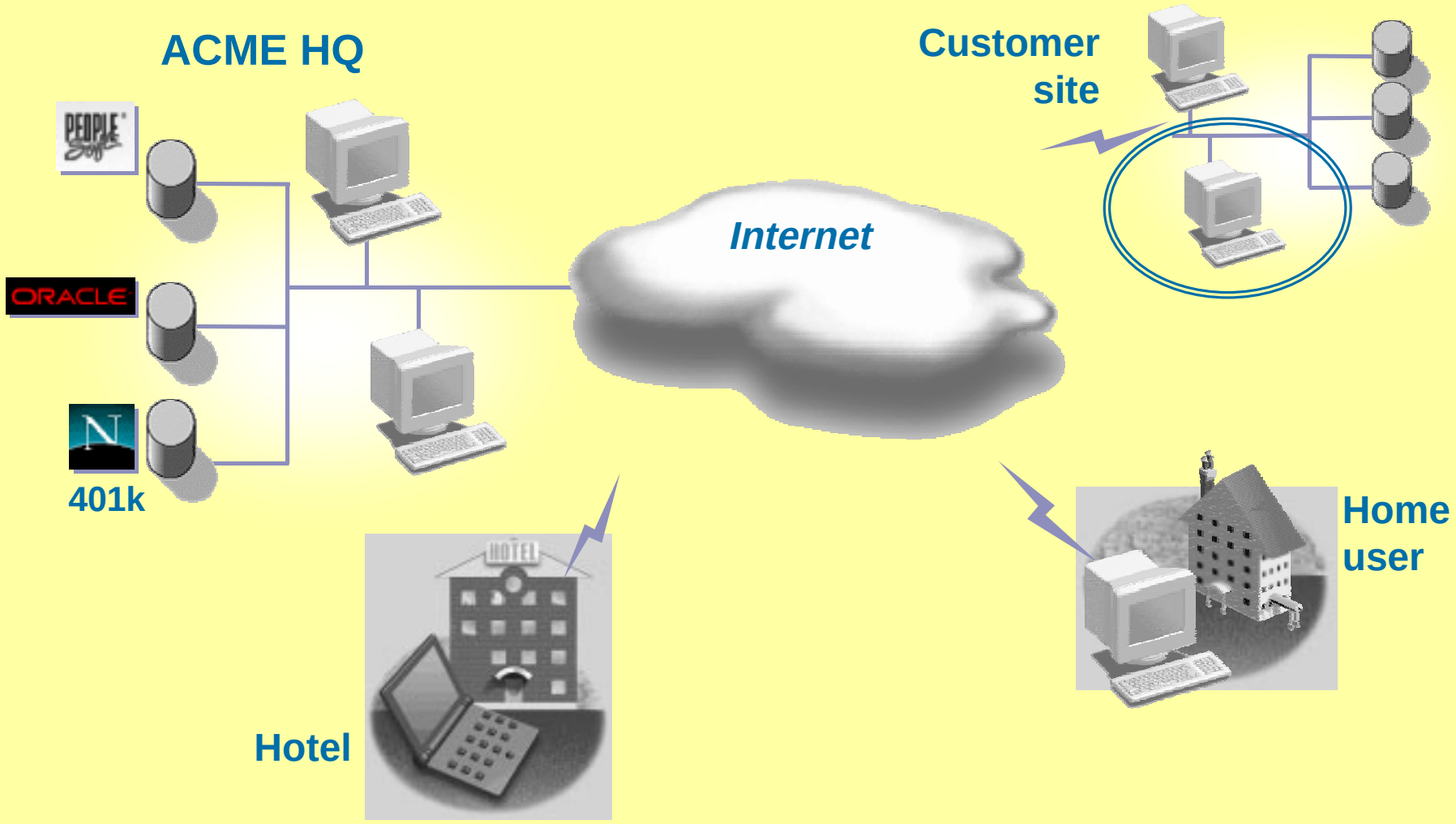
Introducing ACME Conglomerate

- **The Challenge:**
  - **Increase workforce productivity and inter-company collaboration**
- **The Opportunity:**
  - **Utilize powerful ERP software**
  - **Harness the power of the ubiquitous, low-cost Internet backbone**

ACME Conglomerate - The Solution

- Implement PeopleSoft
- Provide mobile communications technology to a worldwide workforce
- Provide access to corporate network and applications via dial-up ISP connections

The Expanded Virtual Network



The Business Benefits

- **Increased employee productivity**
  - **Instant access to critical information, regardless of location**
  - **Enhanced worldwide communication**
  - **Improved employee morale**
- **Reduced facilities costs**
  - **Work from home**
  - **“Hoteling”**

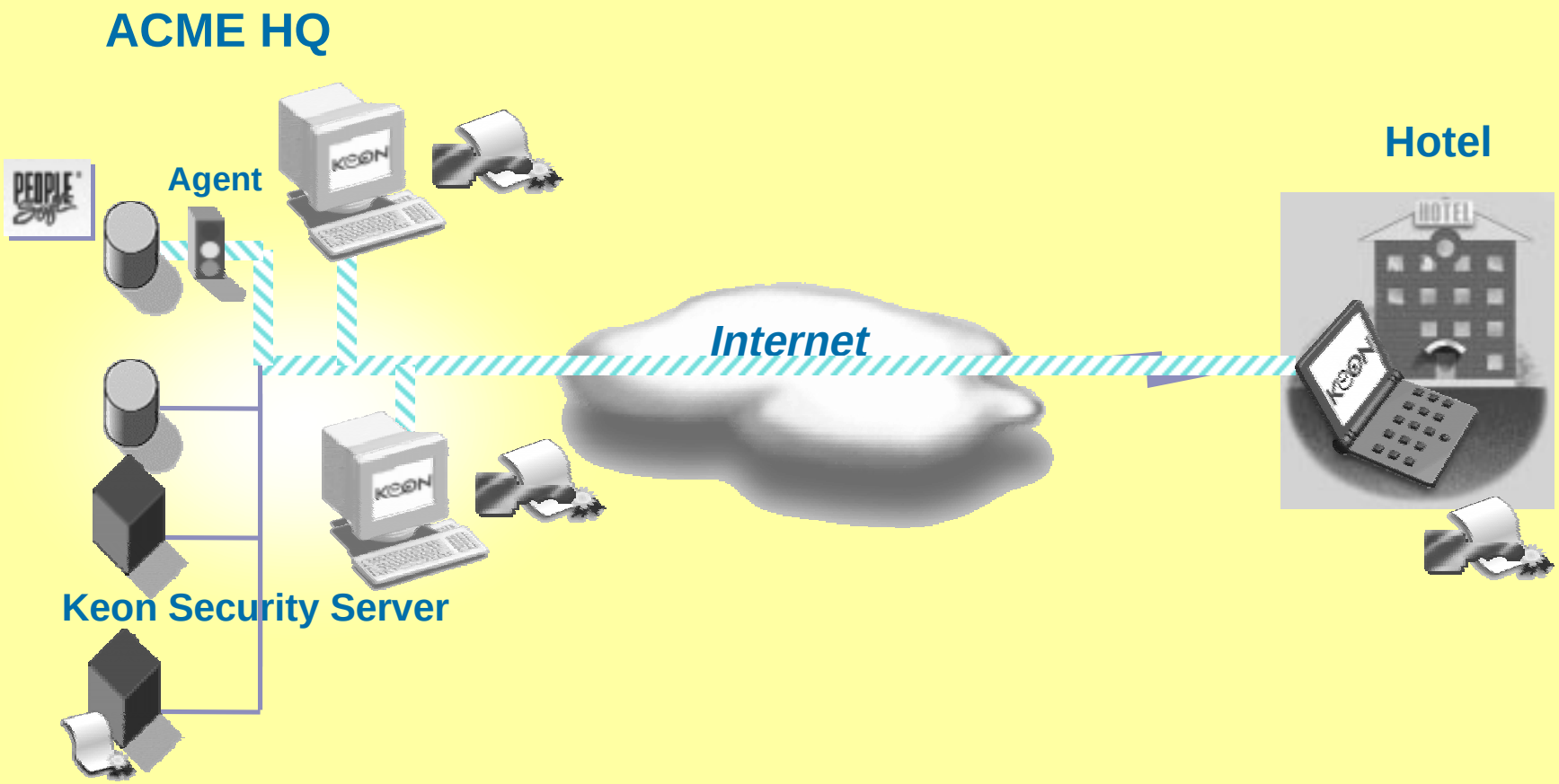
Secure Business Process Requirements

- Maintain confidentiality of data transmitted over the *Internet*
- Maintain confidentiality of data transmitted over the *intranet*
- Know who is accessing confidential business information
- Protect confidentiality of information in local file stores

Protects Data Confidentiality

- Application VPN - from the desktop to the application
  - For all users, Internet & intranet
- No modifications to the application
- Transparent, at network layer
- Industry standard, 128-bit SSL encryption

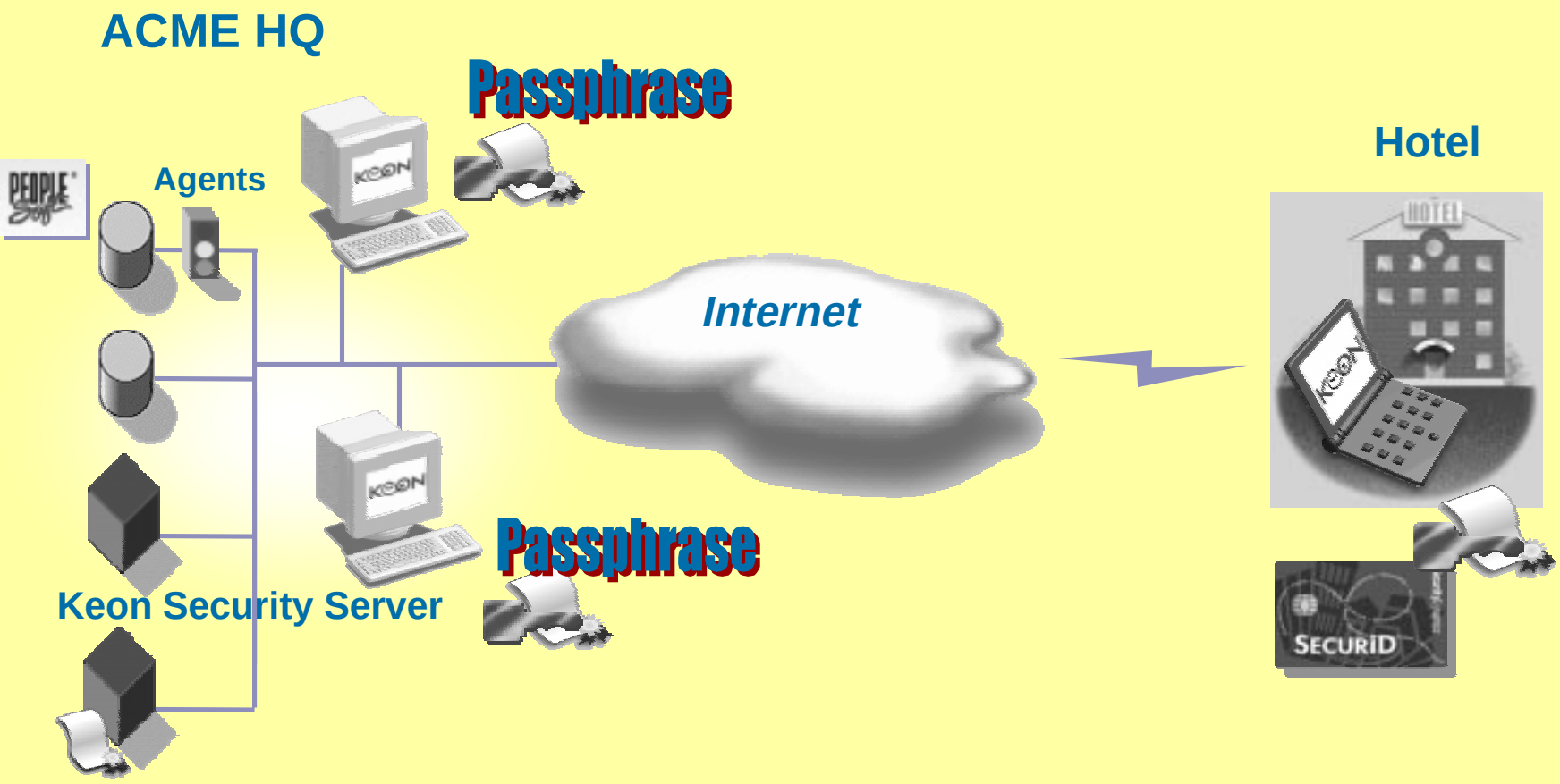
Strong SSL Encryption



Policy-Based Authentication

- Protects digital credentials with choice of passphrase or SecurID strong authentication
  - Passphrase policy management tools at the Keon Desktop
- Multiple strong authentication alternatives
  - SecurID Smart Card
  - SecurID time-synchronous Hardware Token or Key Fob
  - SecurID Software for Palm computer

Policy-Based Authentication



Protects Local Data Stores

- On-the-fly encryption and decryption of local files
  - All files stored in identified directories are automatically encrypted when saved
  - User can specify individual files
- Enables users to send encrypted files to any user

Reduced Sign-on

- Single sign-on to any “Keon-Ready” application
  - PKI-Ready applications
  - Applications protected by Keon Agent
  - NT or NetWare
  - Encrypted local file store
- User authenticates once to their credential store
  - All further access is transparent to user

Keon's Benefit to ACME Conglomerate

- Confidentiality of confidential data over the extended network
- Policy-based user authentication
- Local file store encryption
- Reduced sign-on to multiple applications, encrypted local data store & network environment

Additional Keon Services

Optional Keon UNIX Platform Security

Browser-based Secure UNIX Account Management

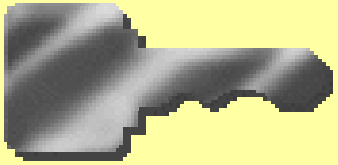
- Secures underlying server platform
- Role-based user management
- UNIX security analysis
- Sophisticated user access control
- Protects UNIX users with SecurID tokens
- Centralized system admin, monitoring and logging

SecurID and Keon
Strong User Authentication

Authentication and Digital Credentials

"Certificates . . . do not address a fundamental problem: authentication. Because access to the certificate is generally based on user ID and pass phrase, an interloper with access to a user's workstation and with knowledge of the person's user ID and pass phrase could masquerade as that user. Accordingly, applications that require higher levels of safety need tokens and biometrics."

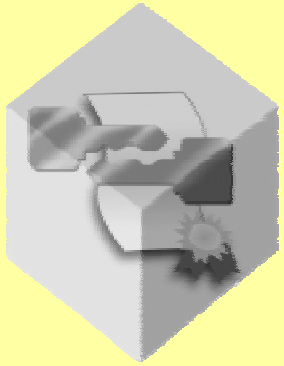
Gartner Group



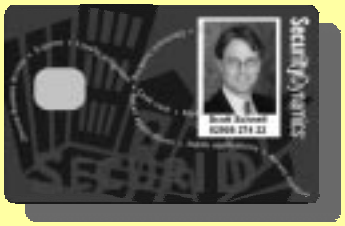
How Secure is the Private Key?

Where is it stored?

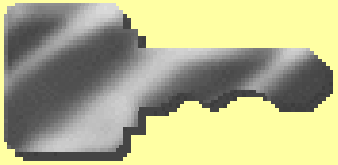
Local Store



Virtual Smart Card



Smart Card

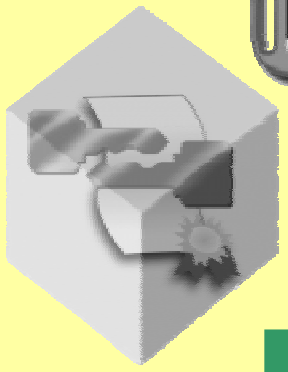


How Secure is the Private Key?

How do you know the private key is being used by its rightful owner?

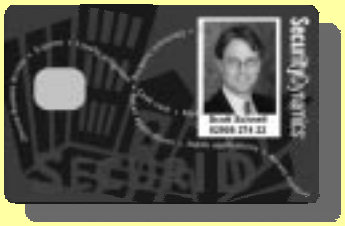
Password

Local Store



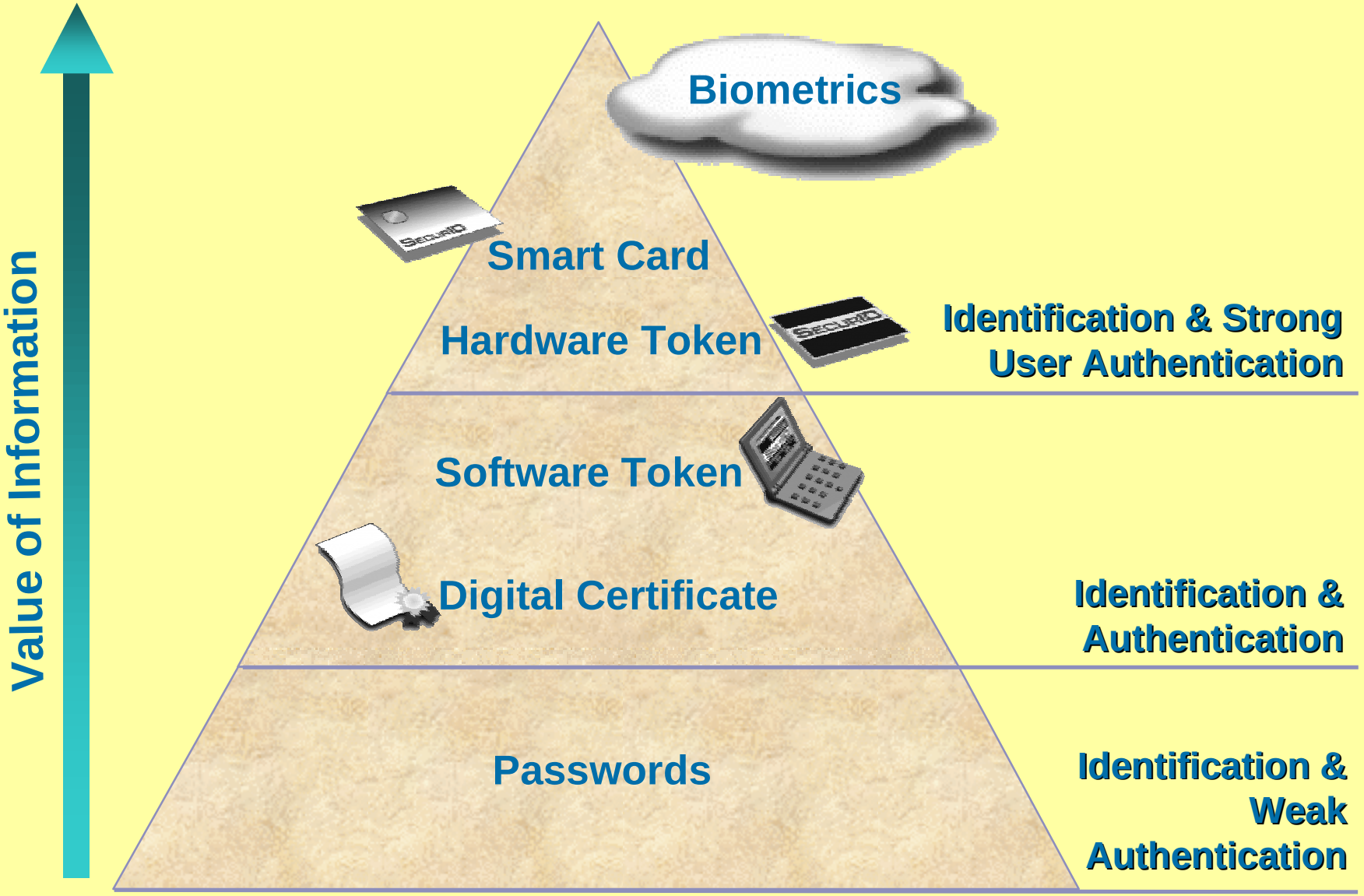
Virtual Smart Card

PIN



Smart Card

Policy Based Authentication



Resolving the Issues

- Multiple sources for certificates
  - support for third party CAs
- Multiple applications need to access certificates … simultaneously
  - PKCS11 and CSP provide support:

    Netscape SSL and S/Mime

    Microsoft SSL (Secure Web Access) and S/Mime (Secure Electronic Mail)

Resolving the Issues (cont.)

- Distributing certificates to users
  - dynamic download of credentials
    - caching under policy control
    - physical transfer if required
- Integrating applications into PKI
  - Keon PKI agents use PAC to make apps PKI aware
- Certificates and authentication
  - support for virtual and physical smart card


KEON
POWERED BY RSA™